ISSN 2072-8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА. СУДОВА ЕКСПЕРТИЗА. ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.14

Степанов Валерій Анатолійович,
кандидат технічних наук, науковий співробітник
ІСТЕ СБ України, м. Київ, Україна,
ORCID ID 0000-0002-5249-6883
Челпан Юрій Васильович,
провідний науковий співробітник
ІСТЕ СБ України, м. Київ, Україна,
ORCID ID 0009-0007-3540-6421

АСПЕКТИ ЗАКОННОГО ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ

У статті наведено ідентифікаційні ознаки об'єктів перехоплення у мережах мобільного зв'язку п'ятого покоління 5G: SUPI, SUCI, PEI, GUTI та GPSI. Встановлено, що модулі ядра мережі 5G: AMF, SMF, UDM, SMSF, UPF та NEF мають взаємодіяти зі шлюзом мережного комплекту технічних засобів системи перехоплення інформації. Вказано, що засоби управління та обробки технічних засобів системи перехоплення інформації мають отримувати від постачальників послуг електронних комунікацій дані щодо асоціації ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI. Акцентовано увагу на появі нового інтерфейсу HI4.

Ключові слова: *законне перехоплення, електронна комунікаційна мережа, ідентифікаційні ознаки, мобільний зв'язок, технічні засоби.*

Постачальники послуг електронних комунікацій в Україні розпочали впровадження технології мобільного зв'язку п'ятого покоління 5G. Технологія 5G, як і технології попередніх поколінь 3G/4G та функції законного перехоплення інформації (Lawful Interception) з мереж мобільного зв'язку вказаних поколінь, стандартизована Партнерським проєктом третього покоління (3GPP) та Європейським інститутом телекомунікаційних стандартів (ETSI). Відмінності технології 5G та бізнес-сценаріїв, що реалізуються в мережах 5G, від технологій 3G/4G та вже упроваджених у бізнес проєктів природно викликають необхідність у модернізації технічних засобів для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України (далі – технічних засобів), вимоги до яких наведено в нормативному документі [1].

Зазначені технічні засоби досліджували С.М. Грищенко, О.В. Манжай, Ю.М. Парасіч, С.В. Пеньков, І.К. Стішенко [2–5] та ін. У більшості наукових праць і прикладних

робіт досліджувались теоретичні та нормативні аспекти побудови технічних засобів щодо технологій мобільного зв'язку поколінь 2G, 3G, 4G. Праці зазначених науковців прикладних установ та роботи фахівців уповноважених органів безсумнівно є вагомим внеском у дослідження вказаних технічних засобів. Отримані результати потребують всебічного осмислення, систематизації й подальшого вдосконалення науковцями та фахівцями різних профілів знань у контексті застосування як єдиної системи технічних засобів [2], так і вузькопрофільних технічних засобів [3]. Однак донині загальні вимоги до технічних засобів щодо технології мобільного зв'язку покоління 5G не сформовано.

Метою статті є формування пропозицій для внесення змін до нормативного документа [1] на основі опрацювання технічних специфікацій 3GPP та ETSI щодо законного перехоплення інформації в мережах мобільного зв'язку покоління 5G.

Розглянемо чотири аспекти законного перехоплення інформації в електронних комунікаційних мережах мобільного зв'язку п'ятого покоління.

По-перше, поява нових ідентифікаційних ознак об'єктів перехоплення. У технічній специфікації ETSI TS 133 127 [6] наведено ознаки об'єктів перехоплення (ідентифікатори), що використовують під час роботи мережі мобільного зв'язку покоління 5G: спеціально введені SUPI (subscriber permanent identity), GUTI (globally unique temporary identity), SUCI (subscription concealed identifier), PEI (permanent equipment identifier), GPSI (generic public subscription identifier) та раніше відомі IMSI (international mobile subscriber identity), MSISDN (mobile subscriber integrated services digital network number), IMEI (international mobile equipment identity), NAI (network access identifier), SIP – URL (session initiation protocol – uniform resource locator), TEL-URL (telephone link protocol – uniform resource locator), IMPU (IP multimedia public user identifier), IMPI (IP multimedia private identity).

Для постійної ідентифікації користувача (споживача) послуг зазначеної мережі введено ознаку SUPI. Постачальник послуг надає цю унікальну ознаку (ідентифікатор) кожній SIM-карті. У попередніх поколіннях мереж мобільного зв'язку аналогом SUPI була міжнародна ідентифікаційна ознака користувача послуг мобільного зв'язку IMSI. Щоб уникнути порушення конфіденційності під час автентифікації користувача послуг відвідувана мережа призначає SIM-карті тимчасові ідентифікаційні ознаки користувача послуг мобільного зв'язку TMSI (temporary mobile subscriber identity) в мережах поколінь 2G, 3G та глобальні унікальні тимчасові ідентифікаційні ознаки GUTI в мережах поколінь 4G, 5G. Ознаки 5G-GUTI часто змінюються та використовуються з метою ідентифікації через радіоканал. Проблема конфіденційності через атаки перехоплення IMSI в мережах мобільного зв'язку поколінь 2G, 3G та 4G протягом десятиліть залишалася не вирішеною. Однак у поколінні 5G 3GPP вирішив цю проблему, хоча й шляхом зворотної сумісності. У разі помилки під час ідентифікації через 5G-GUTI, на відміну від попередніх поколінь, технічні специфікації 5G не дозволяють передавати SUPI у відкритому вигляді радіоканалом. Замість цього передається ідентифікаційна ознака захисту конфіденційності на основі інтегрованої схеми шифрування еліптичної кривої (ECIES) з відкритим ключем домашньої мережі, безпечно наданим під час реєстрації. Така прихована ознака SUPI відома як прихована ідентифікаційна ознака користувача

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

послуг SUCI, що генерується обладнанням користувача послуг. У мережах мобільного зв'язку покоління 5G технічними специфікаціями 3GPP також визначено постійну ідентифікаційну ознаку обладнання PEI для обладнання (термінала) користувача послуг. За допомогою PEI вказана мережа ідентифікує обладнання користувача послуг, що здатне отримати доступ до неї. Водночас PEI може приймати різні формати для різних типів обладнання користувача послуг та варіантів використання. Обладнання користувача послуг має подати PEI в мережу разом із зазначенням формату, що використовується. Якщо обладнання користувача послуг підтримує одну технологію доступу, йому має бути призначено PEI у форматі міжнародного ідентифікатора обладнання IMEI. З метою організації технічними засобами законного перехоплення представляє інтерес розгляд загальної відкритої ідентифікаційної ознаки користувача послуг GPSI, яка використовується у технічних специфікаціях 3GPP щодо мереж покоління 5G, так і поза ними. Ця ідентифікаційна ознака є ідентифікатором загального користування, таким як міжнародний номер користувача послуг мобільного зв'язку MSISDN, або зовнішнім ідентифікатором. При цьому в мережах покоління 5G зберігається асоціація між GPSI та відповідним SUPI.

По-друге, поява нових функціональних модулів у ядрі мережі 5G (5G Core Network). До складу мережного комплекту технічних засобів відповідно до нормативного документа [1] входять шлюз (точка доступу в електронній комунікаційній мережі) та обладнання відбору об'єктів перехоплення (пункти доступу). У наведеній вище технічній специфікації ETSI TS 133 127 [6] згідно зі схемою ядра мережі 5G (5G Core Network) до обладнання відбору об'єктів перехоплення належать такі модулі:

1) AMF (core access and mobility management function) – мережної функції управління доступом та мобільністю;

2) SMF (session management function) – мережної функції управління сеансами користувачів послуг;

3) UDM (unified data management) – управління даними користувачів послуг на основі уніфікованої бази даних його профілів;

4) SMSF (SMS function) – функції підтримки обміну короткими текстовими повідомленнями через протокол NAS;

5) UPF (User Plane Function) – функції площини передачі даних користувачів послуг;

6) NEF (network exposure function) – функції забезпечення взаємодії з зовнішніми платформами та додатками.

Модулі AMF, SMF, UDM, SMSF, UPF, NEF генерують та надають до шлюзу службові дані сеансів зв'язку абонентів спостереження IRI (intercept related information), що використовуються для встановлення, підтримання та закінчення сеансу зв'язку, замовлення та відміни основних, додаткових послуг, та дають змогу ідентифікувати електронну комунікаційну мережу, електронну комунікаційну послугу й кінцеве (термінальне) обладнання, його місцезнаходження і належність.

Модулі UPF та NEF, крім IRI, також надають до шлюзу інформаційні повідомлення сеансів зв'язку абонентів спостереження CC (content of communication), що включають у себе IP-сеанси голосових повідомлень і розмов у форматі PCAP-файлів.

DOI (Article): https://doi.org/10.36486/np.2024.3(65).18

Зауважимо, що тільки два модулі UPF та NEF надають до шлюзу повну інформацію про вміст сеансів зв'язку абонентів спостереження.

У модулях AMF, SMF, UDM, SMSF, UPF і NEF здійснюються спостереження за сеансами користувачів послуг (абонентів спостереження) та їх відбір за визначеними ідентифікаційними ознаками, зокрема SUPI, PEI та GPSI з подальшою доставкою до шлюзу. Схема загальна законного перехоплення інформації в мережі 5G наведена на рисунку 1.

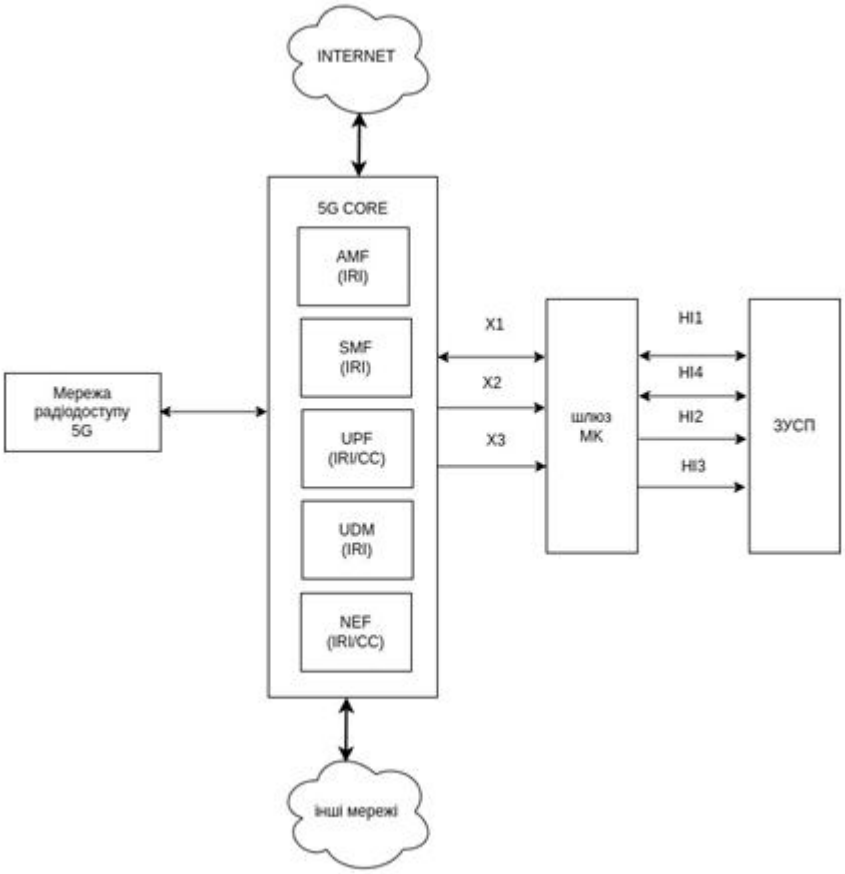

Рис. 1. Схема загальна законного перехоплення інформації в мережі 5G

По-третє, поява нових асоціацій ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI. У додатку Г нормативного документа [1] вказано про необхідність надання постачальниками електронних комунікаційних мереж та/або послуг до засобів управління системою перехоплення уповноваженого органу (далі – ЗУСП) службових даних електронних комунікацій та збережених ними протягом строку позовної давності, визначеного законом, записів про надані комунікаційні послуги. Наведена вище інформація, у тому числі асоціації ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI використовується в ЗУСП для організації

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

перехоплення електронних комунікацій та для кореляції (зіставлення) ідентифікаційних ознак, за якими здійснюється перехоплення електронних комунікацій з ознаками, що містяться в IRI відгалужених сеансів зв'язку користувачів послуг (абонентів спостереження).

По-четверте, поява в технічних специфікаціях ETSI TS 133 127 [6] та ETSI TS 133 128 [7] нового інтерфейсу управління та передавання HI4 взаємодії шлюзу мережного комплекту з ЗУСП. Згідно із зазначеними специфікаціями під час використання інтерфейсу HI4 зі шлюзу до ЗУСП передаються дані стану законного перехоплення.

За результатами наведених аспектів законного перехоплення інформації в електронних комунікаційних мережах мобільного зв'язку п'ятого покоління вважаємо за доцільне запропонувати такі зміни в нормативному документі [1]:

1) врахувати появу нових ідентифікаційних ознак об'єктів перехоплення SUPI, GUTI, SUCI, PEI та GPSI;

2) шлюз має бути з'єднаним з обладнанням відбору об'єктів перехоплення – функціональними модулями мережі мобільного зв'язку 5G: AMF, SMF, UDM, SMSF, UPF, NEF та за внутрішніми інтерфейсами має надавати до вказаних модулів таблицю спостереження з ідентифікаційними ознаками об'єктів перехоплення, а також отримувати від них метадані щодо IRI та інформаційні дані щодо CC відібраних сеансів зв'язку абонентів спостереження;

3) ЗУСП має отримувати інформацію щодо асоціацій ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI за інтерфейсом запиту та доставки службових даних;

4) у разі побудови шлюзу за технічними специфікаціями ETSI необхідно зважати на появу інтерфейсу HI4.

Запропоновані пропозиції рекомендуємо використовувати під час підготовки нормативно-правових актів із законного перехоплення інформації в Україні та нової редакції нормативного документа [1], а також під час планування оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах мобільного зв'язку покоління 5G.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України. Загальні технічні вимоги: наказ Служби безпеки України і Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 31.12.2021 р. № 460/781. URL: https://ssu.gov.ua/uploads/documents/2022/01/24/ztv-31122021.pdf (дата звернення: 12.06.2024).

2. *Степанов В.А., Грищенко С.М.* Єдина система технічних засобів зняття інформації з електронних комунікаційних мереж: зб. наук. пр. НАСБУ. 2021. № 78. С. 211–215.

3. *Степанов В.А., Грищенко С.М.* Технічні засоби для негласного зняття інформації з електронних комунікаційних мереж. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2021. № 4. С. 280–284. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2022/02/NV4/Макет_НВ_4_2021_мягк-280-284.pdf (дата звернення: 12.06.2024).

DOI (Article): https://doi.org/10.36486/np.2024.3(65).18

4. *Парасіч Ю.М.* Використання можливостей DPI-систем для організації законного перехоплення на магістральних каналах зв'язку: зб. наук. пр. НАСБУ. 2017. № 65. С. 239–244.

5. *Степанов В.А., Стішенко І.К.* Особливості дозволеного законом перехоплення інформації з телекомунікаційних мереж. *Спеціальні телекомунікаційні системи та захист інформації.* 2005. № 10. С. 76–80.

6. ETSI TS 133 127 V17.5.0 (2022-07) Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Lawful Interception (LI) architecture and functions. URL: https://www.etsi.org/deliver/etsi_TS/133100_133199/133127/17.05.00_60/ts_133127v170500p.pdf (дата звернення: 12.06.2024).

7. ETSI TS 133 128 V16.5.0 (2021-01) LTE; 5G; Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Security; Protocol and procedures for Lawful Interception(LI). URL: https://www.etsi.org/deliver/etsi_ts/ 133100_133199/133128/16.05.00_60/ts_133128v160500p.pdf (дата звернення: 12.06.2024).

REFERENCES

1. Tehnichni zasoby dlia zdiisnennia upovnovazhenymy orhanamy operatyvno-rozshukovyh, kontrrozviduvalnykh, rozviduvalnyh zakhodiv ta nehlasnyh slidchykh (rozshukovykh) dii v elektronnykh komunikatsiinykh merezhakh zahalnoho korystuvannia Ukraini. Zahalni tekhnichni vymohy. "Technical means for the implementation by authorized equipment's of operative-search, counter-intelligence, reconnaissance measures and covert investigative (search) actions in electronic communication networks of public use in Ukraine. General technical requirements": Order of the Security Service of Ukraine and the Administration of the State Service for Special Communications and Information Protection of Ukraine. Dated December 31, 2021 No. 460/781. URL: ssu.gov.ua/uploads/documents/ 2022/01/24/ztv-31122021.pdf. (Date of Application: 12.06.2024) [in Ukrainian].

2. *Stepanov, V.A., Hryshchenko, S.M.* (2021). Yedyna systema tehnichnykh zasobiv zniattia informatsii z elektronnykh komunikatsiinykh merezh. "A unified system of technical means of lawful interception from electronic communication networks": *Collection of scientific works of the National Academy of the Security Service of Ukraine. No. 78.* P. 211-215 [in Ukrainian].

3. *Stepanov, V.A., Hryschenko, S.M.* (2021). Tekhnichni zasoby dlia nehlasnoho zniattia informatsii z elektronnykh komunikatsiinykh merezh. "Technical means for covert removal of information from electronic communication network": *Scientific Bulletin of the Dnipro State University of Internal Affairs, 4,* 280-284. URL: https:visnik.dduvs.in.ua/wp-content/uploads/2022/02/NV4/Макет_НВ_4_2021 _мягк-280-284.pdf. (Date of Application: 12.06.2024) [in Ukrainian].

4. *Parasich, Yu.M.* (2017). Vykorystannia mozhlyvostei DPI-system dlia orhanizatsii zakonnoho perekhoplennia na mahistralnykh kanalakh zviazku. "Using the capabilities of DPI systems to organize lawful interception on backbone communication channels": *A collection of scientific papers of the National Academy of the Security Service of Ukraine. No. 65.* P. 239-244 [in Ukrainian].

5. *Stepanov, V.A., Stishenko, I.K.* (2005). Osoblivosti dozvolenohho zakonom perekhoplennia informatsii z telekomunikatsiinykh merezh. "Peculiarities of lawful interception of information from telecommunication networks": *Special Telecommunication Systems and Information Protection, 10,* 76-80 [in Ukrainian].

6. ETSI TS 133 127 V17.5.0 (2022-07) Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Lawful Interception (LI) architecture and functions. URL: https://www.etsi.org/deliver/etsi_TS/133100_133199/133127/17.05.00_60/ts_ 133127v170500p.pdf. (Date of Application: 12.06.2024) [in English].

7. ETSI TS 133 128 V16.5.0 (2021-01) LTE; 5G; Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Security; Protocol and procedures for Lawful Interception(LI).URL: https://www.etsi.org/deliver/etsi_ts/133100_133199/133128/16.05.00_60/ts_133128v160500p.pdf. (Date of Application: 12.06.2024) [in English].

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

UDC 343.14

Stepanov Valerii,
Candidate of Technical Sciences,
Researcher of the Ukrainian Research Institute of Special Technology and Forensic Expertise of the Security Service of Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0002-5249-6883
Chelpan Yurii,
Leading Researcher of the Ukrainian Research Institute of Special Technology and Forensic Expertise of the Security Service of Ukraine, Kyiv, Ukraine,
ORCID ID 0009-0007-3540-6421

ASPECTS OF LAWFUL INTERCEPTION OF INFORMATION IN FIFTH GENERATION MOBILE COMMUNICATION NETWORKS

The article examines four aspects of lawful interception of information in electronic communication networks of fifth generation mobile communication 5G. This article sets out to outline the identification features SUPI, SUCI, PEI, GUTI and GPSI of interception objects in the specified networks. Furthermore, it describes the scenarios of their use during the lawful interception of information, as set out in the ETSI technical specifications. The authors established that the AMF, SMF, UDM, SMSF, UPF and NEF modules of the 5G-core network must interact with the network gateway of the technical means of the interception system. It is indicated that the means of control and processing of the technical means of the information interception system must receive data on association of identification features of interception objects SUCI with SUPI and 5G-GUTI with SUPI from service providers of electronic communications. This study places particular emphasis on the emergence of a novel control and handover interface, designated HI4, within the ambit of the ETSI technical specification. This paper puts forward a series of recommendations for amendments to the normative document on lawful interception in Ukraine. The proposal is recommended for use during the planning of operative-search, counterintelligence, reconnaissance measures, and covert investigative (search) actions in 5G mobile communication networks of public use in Ukraine.

Keywords: lawful interception, electronic communication network, identification features, mobile communication, technical means.

Отримано 01.08.2024